



Annex 1: Internal Instruction on AML/CFT Procedures

VoltEnt B.V.

Version 2.0 | May 2025

Approved by: Michał Ziobro

Date: May 1st 2025

Next Review Date: May 1st 2026

Any revisions shall be approved by the Compliance Officer or Company Director and communicated company-wide.

1. General Provisions

This Internal Instruction defines the operational procedures adopted by VoltEnt B.V. ("Company") to counteract money laundering (ML), the financing of terrorism (TF), and proliferation financing (PF). This Instruction forms an integral part of the Company's AML/CFT Policy and outlines procedures to ensure compliance with applicable regulations and supervisory expectations in Curaçao.

The obligation to adopt and apply this Instruction derives from the following sources:

- **National Ordinance on the Reporting of Unusual Transactions (NORUT)**
- **National Ordinance on the Identification of Clients (NOIS)**
- **Sanctions National Ordinance**
- **Kingdom Sanction Law (Rijkssanctiewet)**
- **Central Bank of Curaçao AML/CFT/CFP Guidelines for Factoring Companies (August 2023)**
- **Relevant FATF Recommendations and guidance papers**
- **Applicable guidance from the Basel Committee on Banking Supervision**

The objective of this Instruction is to ensure that VoltEnt B.V.:

- Implements sound AML/CFT internal control procedures;
- Minimizes the risk of misuse of its products and services for unlawful activities;
- Protects the integrity and reputation of the Company and the financial system of Curaçao.

This Instruction applies to all business units and employees involved in onboarding, monitoring, or managing customer relationships and transactions.

2. Definitions

For the purposes of this Instruction:

Real Beneficiary – A natural person who ultimately controls a client (directly or indirectly), owns more than 25% of shares/voting rights, or exercises control through other means. For trusts: includes founder, trustee, beneficiaries, or persons with equivalent control. For individuals with no indications of external control, they are assumed to be the real beneficiary.

Politically Exposed Person (PEP) – High-level public officials (e.g., heads of state, ministers, MPs, judges, central bank members, ambassadors, senior military, executives in state-owned companies, etc.).

Family Members of a PEP – Spouse/partner, children (and their partners), and parents.

Close Associates of a PEP – Persons with joint beneficial ownership or known close business ties with a PEP.

Senior Management – Individuals in a company with knowledge and decision-making authority regarding AML risks.

Client – Any person or entity receiving services or engaging in transactions with an obligated institution.



Sanction Lists – Lists of individuals/entities subject to financial or legal restrictions, including EU and national listings.

Non-Disclosure of Assets – A restrictive measure prohibiting making assets available to sanctioned persons/entities.

Money Laundering – As defined by the relevant AML laws.

Business Relationship – Ongoing professional engagement between a client and institution.

Transaction – Any act involving the transfer of ownership or possession of property values.

Occasional Transaction – One-off transaction outside a business relationship.

Related Transaction – Multiple smaller transactions totaling over €15,000, linked to avoid detection.

Suspicious Transaction – Any transaction possibly linked to money laundering or terrorist financing.

Transfer of Funds – Electronic transfer of money via a payment provider, regardless of sender/recipient identity.

Trust – A legal arrangement transferring assets to a trustee for the benefit of others.

Property Values – Includes assets, payment means, securities, financial instruments, and virtual currencies.

3. Identification and Verification Procedures

VoltEnt B.V. shall identify and verify the identity of all clients prior to:

- Establishing a business relationship;
- Conducting an occasional transaction amounting to at least EUR 15,000 (or its equivalent);
- Suspecting ML/TF;
- Doubting the veracity or adequacy of previously obtained client identification data.

Procedures include:

- Collection and verification of reliable and independent source documents;
- Identification of UBOs in line with NOIS requirements and risk profile of the client;
- Sanctions screening against UN, EU, and Curaçao lists prior to account activation;
- Refusal or termination of relationship if CDD requirements cannot be fulfilled;
- For high-risk clients and PEPs: enhanced due diligence (EDD) must be applied.

Client and Beneficial Owner Identification

1. Client Identification

The employee handling client onboarding or cooperation must collect and record the following:

- **For legal entities:**
 - Name, legal form, business address, tax ID (or registration details if no tax ID),
 - Details of the representative: full name, ID number or date and country of birth.
- **For natural persons:**
 - Full name, citizenship, ID number or date and country of birth,
 - Identity document details, residence address (if available),
 - If conducting business: business name, tax ID, and business address.
- **For authorized representatives:**
 - Full name, citizenship, ID number or date and country of birth,
 - Identity document details and residence address.

2. Verification

Data must be verified using appropriate documents, such as:

- Registration or ID documents,
- Licenses or permits,
- Company statutes or contracts,
- Notarial documents,
- Reliable internal or public databases.

3. Beneficial Owner Identification

The Company must identify and verify the client's beneficial owner by recording:

- Full name, citizenship, and if available: ID number or date and country of birth, identity document details, and address.



Verification is based on a **Beneficial Owner Declaration**, official registers (e.g. KRS), or credible sources

4. Risk Assessment and Classification

A documented ML/TF risk assessment must be conducted at onboarding and reviewed periodically. Clients shall be classified into risk categories (low, medium, high) based on:

- Type of client and its ownership/control structure;
- Geographic risk (e.g., clients from jurisdictions listed by FATF);
- Delivery channels and nature of products/services;
- Historical transaction behavior and linkages to higher-risk sectors.

Enhanced due diligence shall be applied where the risk is assessed as high. The risk assessment must reflect Curaçao's National Risk Assessment outcomes and be consistent with the Central Bank's expectations.

5. Ongoing Monitoring

The Company shall implement appropriate financial security measures as part of its risk-based approach to AML compliance. These include:

- **Identifying and verifying the identity** of clients, including natural persons, legal entities, and organizational units;
- **Identifying the ultimate beneficial owner (UBO)** and taking reasonable steps to verify their identity and understand the ownership and control structure in the case of legal persons or similar arrangements;
- **Assessing the purpose and intended nature** of the business relationship, especially for higher-risk clients;
- **Ongoing monitoring** of the business relationship, including:
 - Reviewing transactions to ensure they align with the Company's knowledge of the client's profile and business activities;
 - Examining the source of funds where circumstances indicate a higher risk;
 - Ensuring all client documentation, data, and KYC records are current and accurate.

These measures must be applied:

- At the start of any new business relationship;
- When there is suspicion of money laundering or terrorist financing, regardless of the transaction amount;
- Whenever doubts arise regarding the accuracy or completeness of client identification data;
- In the provision of services such as bookkeeping, tax filings, or advisory in tax/customs law.

Any unusual findings or inconsistencies during ongoing monitoring must be promptly escalated to the Compliance Officer.

6. Suspicious Transaction Reporting (STR)

All employees must remain vigilant to the risk of money laundering or terrorism financing. When a transaction meets indicators of suspicion or matches a red flag, employees must:

- Immediately report to the Compliance Officer;
- Provide all supporting documents and rationale for suspicion;
- Not inform the client (prohibition on tipping off);
- Cooperate with FIU Curaçao and competent authorities as required.

The Compliance Officer is responsible for determining whether a formal STR is submitted to FIU Curaçao in line with NORUT.

7. Terrorist Financing: Sources and Transfer Methods

Common sources of terrorist financing include:



- Misuse of non-profit organizations (e.g., charities, foundations, religious associations) for fundraising or as fronts;
- Revenues from legitimate small businesses, especially cash-intensive ones (e.g., restaurants, workshops);
- Criminal activity such as drug trafficking, fraud, extortion, or smuggling;
- Donations or transfers from state sponsors of terrorism or wealthy individuals;
- Proceeds from natural resources in failed states;
- Members' legal income or social benefits used for self-financing;
- Use of legally acquired funds directed toward terrorism (also known as "reverse laundering").

Terrorist networks use the following transfer methods:

- The formal financial system (e.g., transfers, prepaid cards, cryptocurrencies);
- Physical transport of cash or valuables by couriers or via informal "underground" banking systems;
- International trade-based mechanisms (e.g., over- or under-invoicing of goods such as diamonds).

8. Record-Keeping

In accordance with NOIS and NORUT, the Company shall retain all documents and data relating to:

- Client identification and verification;
- UBO information and supporting declarations;
- Risk classification and CDD/EDD procedures;
- Transactions, internal reports, STRs, and sanctions screenings.

The retention period is a minimum of **6 years** following the end of the business relationship or transaction.

9. Training and Awareness

Training is essential to ensure employees understand their AML/CFT obligations. VoltEnt B.V. shall:

- Provide induction training on AML/CFT obligations to all new employees;
- Organize annual refresher sessions with case studies and updated typologies;
- Maintain attendance logs and evidence of knowledge testing;
- Adapt training programs to the risk exposure of the role.

10. Independent Testing and Audits

The effectiveness of the AML/CFT framework shall be assessed through:

- Annual internal audits by the compliance or audit team (if applicable);
- Independent external reviews if required by the Board or regulator (on demand);
- Review scope must include sample testing of client files, monitoring outputs, training, and STR documentation.

Findings must be reported to senior management, and remediation measures tracked.

11. Review and Amendment

This Instruction shall be reviewed at least once every 12 months or upon:

- Changes in applicable legislation or FATF guidance;
- Material changes to the business model or services offered;
- Recommendations from internal or external audits;
- Supervisory findings or feedback from the Central Bank.